UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

Aimée Sutton, on behalf of herself and all others similarly situated Plaintiff, v. Target Corporation, Defendant.	)	No. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiff Aimée Sutton ("Plaintiff"), individually and on behalf of all others similarly situated, alleges the following against Target Corporation ("Defendant" or "Target"), based upon personal knowledge, where applicable, on information and belief, and the investigation and research of counsel.

II. NATURE OF THE ACTION

1. As the second largest retailer in the United States with over $72 billion in annual retail sales, a massive security breach during the peak of the 2013 holiday season was a risk Target should have foreseen.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

2. Nonetheless, from about November 27 through December 15, 2013, the computer system of Target was breached on an unprecedented scale. In what would soon come to be recognized as the largest broad-scale theft of personal and financial information from a retailer in history, the Target data breach has so far impacted at least 40 million credit card and debit account holders, and at least 70 million individuals whose Personally Identifiable Information ("PII"), including personal and financial data, was compromised.

3. The breach of Target's computer system is all the more remarkable when viewed in the context of the growth of the company. Instead of investing in technology to protect its ever-growing consumer base, Target's focus has been on improving its bottom line. While undertaking what CEO Gregg Steinhafel bragged in his 2013 letter to Target's shareholders to be "the largest, single-year store expansion in Target's history," Target took inadequate steps to safeguard the PII of tens of millions of its consumer "guests" – the primary contributors to Target's success. *See* Target Corporation Annual Report (2012), https://corporate.target.com/_media/TargetCorp/annualreports/content/download/pdf/Annual-Report.pdf?ext=.pdf.

4. Target's website promises a pleasant and secure shopping experience: "When guests shop at Target, they'll find an environment where shopping is convenient and enjoyable." *See* Target, *Fast Facts* (Jan. 13, 2009), http://pressroom.target.com/news/fastfacts. However, in late 2013, instead of a convenient and enjoyable consumer experience, Target's holiday shoppers experienced a nonstop nightmare of uncertainty, expenditures of money and time, and hassles stemming from Target's huge data breach.

5. Making matters worse, Target has neither promptly nor forthrightly presented facts about the data breach to Plaintiff and the Class, which it is required by law to do, but rather

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

has presented information in an untimely, incomplete and piecemeal fashion, replete with vague references and false promises.

6. In fact, on information and belief, numerous members of the Class – even today – are still unaware that their PII, including key financial information and PINs, was compromised in the massive breach, as notifications from financial institutions and Target continue to trickle in to email in-boxes nationwide. PII, as defined by the U.S. Office of Management and Budget, is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Orszag, Peter R., *Memorandum For The Heads Of Executive Departments And Agencies* (June 25, 2010), http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

7. With an eye toward protecting its own bottom line, and in response to consumer furor, Target has recently come forward with well-publicized, half-hearted promises that no harm will come to consumers:

> We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target. Our brand has been built on a 50-year foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target.

Email from President and CEO Greg Steinhafel to Target Consumers (Dec. 20, 2013), attached hereto as Exhibit 1.

8. Target has also touted that it is extending "free" credit monitoring services:

> Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Email from President and CEO Greg Steinhafel to Target Consumers (Jan. 15, 2014), attached hereto as Exhibit 2; *see also* Target Credit Monitoring FAQ, attached hereto as Exhibit 3. However, this relief is illusory. Given the nature of the PII data which was breached, Target's offer of "free" credit monitoring is akin to pressing a snooze button in order to turn off an alarm – the alarm will not stop sounding until it has been actually turned off. In order to ensure their PII is not misused at some later date, consumers will need to monitor their credit reports on an ongoing basis with no known end date in sight.

9. Moreover, Target has extended services to *only one* of three credit reporting agencies. The Federal Trade Commission recommends that it is advisable to receive credit reports from all three of the nationwide credit reporting companies because "they get their information from different sources." *See* Federal Trade Commission, *Consumer Information: Free Credit Reports*, http://www.consumer.ftc.gov/articles/0155-free-credit-reports (last visited Jan. 16, 2014).

10. Further, the "free" credit monitoring service Target is offering fails to even include the all-important credit score. Instead, consumers who sign up for Target's "free" credit monitoring service are confronted with an offer from the credit reporting agency, Experian, to pay *more* to learn their credit score. *See* Experian Credit Report, attached hereto as Exhibit 4. In effect, Target is turning its consumers into Experian consumers – *at the consumers' expense*. Target's free credit monitoring does not amount to relief for Plaintiff and the Class. Rather, it inflicts further economic injury to Plaintiff and the Class, while generating profit for Experian.

11. None of Target's efforts mitigate the fact that Plaintiff and the Class are vulnerable to continuing fraud and abuse today and in the years to come.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

12. On information and belief, Plaintiff and the Class have been harmed in numerous ways, including but not limited to the following:

(1) having their PII, credit card and debit card accounts used for fraudulent purposes and/or exposed to fraud;

(2) ID theft and/or the very real threat of ID theft;

(3) purchasing and/or implementing their own credit scores and ID theft protection;

(4) suffering harm to their credit scores;

(5) enduring the hassle of cancelling automatic card payments;

(6) handling the reissuing of credit and debit cards;

(7) managing withdrawal and purchase limits which were sporadically imposed on compromised accounts; and

(8) the fact that Target's inadequate, incomplete, and tardy response has exacerbated all of the above.

13. In this electronic age, it is standard practice to encrypt sensitive personal and financial information, such as the PII of consumers, to protect the information from both internal and external threats. Defendant's failure to maintain reasonable and adequate security procedures to protect against the loss of control over Plaintiff's and the Class' PII has put Plaintiff and the Class in harm's way. In addition, Plaintiff and the Class have spent and will need to spend considerable time and money to protect themselves as a result of Defendant's conduct.

14. This Complaint addresses the losses that Plaintiff and the Class have endured today, will suffer in the future, and seeks to prevent future data breaches.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

III. JURISDICTION

15. Diversity jurisdiction over this action is established pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million, and there are more than 100 putative class members.

16. This Court has personal jurisdiction over the Defendant because Defendant is licensed to do business in Washington or otherwise conducts business in Washington.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because unlawful practices are alleged to have been committed in this federal judicial district, Plaintiff resides in this district, and Defendant regularly conducts business in this district.

IV. PARTIES

18. Defendant Target Corporation is a Minnesota corporation, headquartered in Minneapolis, Minnesota. Target is the second largest discount retailer in the United States with approximately 1,921 retail stores.

19. Plaintiff Aimée Sutton resides in Seattle, Washington. On December 3, 2013, she used her debit MasterCard and PIN to make a purchase at the Target store in Downtown Seattle, Washington. Ms. Sutton believed that Target would maintain her personal and financial information in a reasonably secure manner and provided her information to Target on that basis. She would not have shopped at Target if she had known it would make her vulnerable to a data breach disclosing her PII.

20. On January 9, 2014, she received a letter via email from her financial institution that stated in relevant part:

> We are emailing you regarding the Target retail stores security breach. Within the next two weeks you will also receive information via regular mail, however, we

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

> wanted to ensure that you received this important information as timely as possible.
>
> As you may have heard, Target retail stores encountered a security breach that compromised cardholder names, card number, and expiration dates on an undisclosed number of credit and debit accounts. BECU was recently notified that your BECU Debit MasterCard® was compromised.
>
> . . .
>
> It is not necessary for you to call us at this time; however, we would appreciate it if you would continue to take the following steps:
>
> 1. Monitor your account
>
> Unless unauthorized activity is observed on your account, your current Debit MasterCard will remain active through February 20th, 2014. We routinely monitor accounts for unusual activity. In addition, we are encouraging you to periodically monitor your account using Online, Mobile and Telephone Banking and call us at the number on the back of your card if you observe any unauthorized activity. If unauthorized charges are observed on your account, [financial institution] may deactivate your Debit MasterCard prior to the above date.
>
> 2. Activate Your New Card
>
> Your new Debit MasterCard and PIN number will arrive in separate envelopes within the next week. Please note that your new card is not active and will require that you perform a PIN transaction at any ATM or business point-of-sale terminal, once your PIN number arrives. It is not necessary for you to contact [financial institution].
>
> 3. Update Recurring Payments
>
> If you have any recurring payments deducted from your existing Debit MasterCard, you will need to provide the business(es) with your new card number once you receive and activate the card.

21. To date, Target has sent Ms. Sutton *no information*, regarding its breach of her PII and financial information.

22. Instead, the burden is placed completely on Ms. Sutton to perform all of the steps outlined above, including monitoring her account, dealing with a debit card that could be inactivated at any time, activating a new card, and updating any recurring payments – to say

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

nothing of monitoring her other accounts, credit monitoring, and other fraud protection efforts – all without the benefit of any information to her from Target.

23. Moreover, Ms. Sutton is an attorney who charges her clients an hourly rate. Taking the recommended precautions in the wake of Target's breach is costing Ms. Sutton more than time; it is literally costing her money.

V. FACTUAL ALLEGATIONS

24. Target's brand promise is "Expect More. Pay Less." With respect to its data breach, little did unwary holiday consumers know they were supposed to expect less and pay more – for years to come.

25. According to its website, Minneapolis-based Target Corporation (NYSE: TGT) operates 1,921 stores – 1,797 in the United States and 124 in Canada – as well as its online store at Target.com. Target Corporation Factcard (last updated Nov. 21, 2013), http://investors.target.com/phoenix.zhtml?c=65828&p=irol-homeProfile.

A. Target's Security Breach Compromised the PII of Millions of Americans

26. On or between November 27, 2013 through December 15, 2013, thieves collected debit card, credit card, and other personal information from Target customers.

27. During a television interview on January 13, 2014, which aired on CNBC's Business Day programming, Target's CEO, Gregg Steinhafel, stated that he first learned about the data breach on December 15, 2013. The following is an excerpt from that interview:

> **BECKY QUICK**: Tell me again. When did you first find out about this? Was it a phone call? Was it someone came into your office? What happened?
>
> **GREGG STEINHAFEL**: Yeah, let me put the—kind of the timetable in context. I found out on Sunday. Sunday was really day one. It was in the morning.
>
> **BECKY**: Sunday. What was the date?

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

GREGG STEINHAFEL: Sunday, December 15th.

CNBC Exclusive, CNBC Transcript: Target Chairman & CEO Gregg Steinhafel Speaks with Becky Quick Today on CNBC (Jan. 13, 2014), http://www.cnbc.com/id/101331335.

28. Target waited almost a full business week, and then only when other organizations had already notified the press, to tell the public what its CEO admitted it had known for a full business week.

29. During that same television interview on January 13, 2014, Gregg Steinhafel confirmed that thieves installed malware onto the company's point-of-sale registers.

30. A few days after the security breach occurred, on December 18, 2013, Target CEO, Gregg Steinhafel, issued a statement that "We are pleased with Target's holiday performance – from guest experience and engagement, to overall results in both in-store and online." See *Target Unveils Last-Minute Deals in Final Stretch of Holiday Season* (Dec. 18, 2013), http://pressroom.target.com/news/target-unveils-last-minute-deals-in-final-stretch-of-strong-holiday-season. Unbelievably, Target's CEO said nothing about the breach, although he had known for at least three days that Target's "guests'" PII had been in the hands of criminals. It is evident that Target preferred instead to focus on its holiday sales performance.

31. Later that same day, also on December 18, 2013, KrebsOnSecurity.com – not Target – disclosed the first report of Target's data breach. Brian Krebs, *Sources: Target Investigating Data Breach*, KrebsOnSecurity.com (Dec. 18, 2013), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

32. Additionally, also on December 18, 2013, American Express – not Target – confirmed Target's data breach and launched its own investigation. *Timeline of Target's Data Breach*, Star Tribune, Jan. 10, 2014, http://www.startribune.com/business/239623131.html.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

33. Further, on December 18, 2013, the Secret Service – not Target – announced that it had begun its own investigation into Target's data breach. *Id*.

34. Not until KrebsOnSecurity, American Express, and the Secret Service had already reported the breach did Target itself finally inform the public – and even then, its announcement was sketchy and failed to reveal the extent of the problem, or how victims should address the breach.

35. Indeed, on December 19, 2013 Target finally officially confirmed a data breach of 40 million customers who shopped at its U.S. stores and stated that it had "identified and resolved the issue." *See Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores* (Dec. 19, 2013), http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

36. KrebsOnSecurity.com reported on December 20, 2013 that the underground market has been flooded with accounts, "selling batches of one million cards and going for anywhere from $20 to more than $100 per card." Brian Krebs, *Cards Stolen in Target Breach Flood Underground Markets*, KrebsOnSecurity.com (Dec. 20, 2013), http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/.

37. Target responded to the breaking news of the security breach on December 20, 2013, offering customers a 10% discount on all items purchased on December 21st and December 22nd, 2013. This offer was not targeted to Plaintiff and the Class specifically. In fact, most Americans had no idea whether their PII had been compromised because they had not yet been informed that they were affected by the data breach. Target's sale appeared to be a publicity stunt and an effort to recoup losses it incurred from bad press during the holidays. *See A Message from CEO Gregg Steinhafel about Target's Payment Card Issues* (Dec. 20, 2013),

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues.

38. Several days later, on December 23, 2013, the United States Department of Justice announced its investigation into the Target data breach. *See Timeline of Target's Data Breach*, Star Tribune, Jan. 10, 2014, http://www.startribune.com/business/239623131.html.

39. Shortly after the Christmas holiday, on December 27, 2013, Target announced that in addition to customer names, credit and debit card numbers, card expiration dates, and embedded codes on the magnetic strip of the cards, debit card PINs were among the data stolen. *See Target Data Security Media Update #4* (Dec. 27, 2013), http://pressroom.target.com/news/target-data-security-media-update-4.

40. Not until January 10, 2014 did Target reveal the breadth of the security breach: personal information, including names, mailing addresses, phone numbers and email addresses of 70 million customers, were exposed during the data breach. *Target Provides Update on Data Breach and Financial Performance* (Jan. 10, 2014), http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance. However, Target stated it did not know how much overlap exists between the original 40 million customers and the 70 million customers affected, indicating that the number could be as high as 110 million customers. Elizabeth Harris et al., *For Target the Breach Number Grows,* N.Y. Times, Jan. 10, 2014, http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0

41. On information and belief, the information stolen from the initial 40 million customers affected by the breach included names, card numbers, expiration dates, and verification or PIN codes.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

42. On information and belief, the information stolen from the 70 million customers affected by the breach included names, mailing addresses, phone numbers, and email addresses.

43. On January 10, 2014, United States Senators, John D. Rockefeller IV and Claire McCaskill, sent a letter to Target asking it to brief the Senate Commerce, Science and Transportation Committee, stating:

> Target's recent incident demonstrates the need for such federal legislation. . . . It has been three weeks since the data breach was discovered, and new information continues to come out. We expect that your security experts have had time to fully examine the cause and impact of the breach and will be able to provide the committee with detailed information.

Letter to Target Chairmen, President and CEO, Gregg Steinhafel from Senators John D. Rockefeller IV and Clair McCaskill (Jan. 10, 2014), http://www.mccaskill.senate.gov/LetterJointJDRMcCaskilltoTargetDataBreach.pdf

44. On January 12, 2014, Reuters reported that the attackers used malware known as a RAM scraper which enables cyber criminals to capture encrypted data as it travels through the live memory of a computer. Jim Finkle et al., *Exclusive: More well-known U.S. Retailer Victims of Cyber Attacks – Sources*, Thomson Reuters (Jan. 12, 2014) http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112.

45. Cyber criminals may have collected debit card, credit card, and other personal information from Target customers who made purchases at the retailer between 2004 and 2013. Clare O'Connor, *Surprise! Target Data Breach Could Include Your Info from Purchases Made a Decade Ago,* Forbes, Jan. 16, 2014, http://www.forbes.com/sites/clareoconnor/2014/01/16/surprise-target-data-breach-could-include-your-info-from-purchases-made-a-decade-ago/?partner=yahootix.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

B. Despite the Fact that Target Was Aware that a Massive Security Breach Might Occur, Target Failed to Safeguard Its Consumers' PII

46. When consumers make credit and debit card purchases at retailers, including Target, the store collects information related to that card including the card holder name, the account number, expiration date, card verification value (CVV), and PIN for ATM/debit cards. It stores this sensitive financial information in its computing system and sends it to financial instructions so it can get paid. Through its reward system ("REDcard"), and online store, Target also collects and stores customer names, mailing addresses, phone numbers, and email addresses.

47. Target's privacy policy states:

> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

Target Corporation Privacy Policy, http://www.target.com/spot/privacy-policy (last visited Jan. 16, 2014).

48. Target's safeguards fall short of industry standards. For example, the PCI Data Security Standard ("PCI DSS") is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of 12 general requirements: (a) install and maintain a firewall configuration to protect cardholder data; (b) do not use vendor-supplied defaults for system passwords and other security parameters; (c) protect stored cardholder data; (d) encrypt transmission of cardholder data across open, public networks; (e) use and regularly update anti-virus software or programs; (f) develop and maintain secure systems and applications; (g) restrict access to cardholder data by business need to know; (h) assign a unique ID to each person with computer access; (i) restrict physical access to cardholder data; (j) track and monitor all access to network resources and cardholder data; (k) regularly test

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

security systems and processes; and (l) maintain a policy that addresses information security for all personnel. *See* PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard Version 2.0* (Oct. 2010) at 5, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

49. The Federal Trade Commission ("FTC") has issued a publication directed to companies like Target entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"), attached hereto as Exhibit 5. In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes. It gives specific information regarding how to detect any breaches. Following is the FTC's recommended protocol.

> Detecting Breaches
>
> To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
>
> Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.
>
> Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
>
> Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
>
> Have in place and implement a breach response plan.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Federal Trade Commission - Bureau of Consumer Protection, *Protecting Personal Information: A Guide for Business*, http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

50. On information and belief, Target failed to correctly put in place the PCI DSS recommended by the FTC, or any equivalent measures, to protect Plaintiff's and Class' PII, which resulted in the compromise of its consumers PII. Moreover, as evidenced in the events described above, Target failed to timely, accurately, and adequately notify its consumers of the breach.

51. Furthermore, given recent similar events in the marketplace, Target knew or should have known that such a security breach was likely and taken adequate precautions to protect consumers' PII.

52. For example, in 2008 another major retailer, TJX Companies, which operates such retail chains as T.J. Maxx, Marshalls, HomeGoods, A.J. Wright, and Bob's Stores with 2000 locations throughout the U.S. and Canada, paid approximately $20 million in damages and over $177 million in credit monitoring services and identity theft insurance to its consumers. Transcript of Fairness Hearing, *In Re TJX Companies Retail Security Breach Litigation*, No. 1838, No. 07-10162 (D. Mass. July 15, 2008), at 4:16-5:5. In this case, TJX consumers sued TJX for damages they sustained resulting from a four-year-long security breach, during which time over 45 million credit and debit cards and nearly half a million personal identification records were compromised. Amended Consolidated Class Action Complaint, *In re TJX Companies Retail Security Breach Litigation*, MDL No. 1838, No. 07-10162 (D. Mass. Jan. 9, 2008), at 3. TJX consumers also alleged that its security measures failed to comply with industry standards and regulations for protecting consumer PII. *Id.* Similar to Target, TJX delayed

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

notification of the security breach over the lucrative holiday season. *Id.* Undoubtedly, Target would have been well aware of the TJX litigation, the consumer PII safeguard issues, and the resulting litigation.

C. Target's "Remedies" are Inadequate

53. Like the inadequate measures that Target had in place which lead to this massive breach, Target's attempt to remedy the situation with a weak and insufficient credit monitoring program through Experian will do nothing but provide consumers with a false sense of security. Among the inadequacies are the following:

- Consumers can only obtain their credit score if they pay Experian for it. Thus, this is really a chance for Experian to prey on Target's data breach victims.
- The effects of compromised PII frequently do not appear until long after the PII has been compromised; and
- The credit monitoring service offered through Experian reflects *only one of the three major credit reporting agencies*.

54. As if losing control of their PII isn't enough, the Washington Attorney General reports that consumers in the state have already experienced numerous scams as a result of Target's data breach. The Attorney General has stated:

> Beware of Target credit monitoring phishing scams to follow.
>
> The Washington State Attorney General's Office (AGO) warns consumers to be on high alert for 'phishing' emails — emails that look like they originate from Target but are actually scams directed at obtaining personal information.
>
> Phishing emails have already appeared offering 'free' Target gift cards and Target-related credit card monitoring. They typically mention 'Target' in an email that directs consumers to a website with the word 'Target' in its URL.
>
> Do not give out personal information to someone who contacts you before going directly to Target's website to confirm the presented information is correct.
>
> The most up-to-date data breach information for consumers can be found on Target's website here: https://corporate.target.com/about/payment-card-issue.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

> There are also helpful frequently asked questions here: https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ.aspx#q6270.

Washington State Office of the Attorney General, CONSUMER ALERT: Target announces additional consumers impacted by data breach, offers free credit monitoring to all shoppers (Jan. 10, 2014), http://www.atg.wa.gov/pressrelease.aspx?id=31738#.UtcPCdJDs1I.

D. Target Requires Consumers to Disclose Their PII but Fails to Protect It Despite Assurances

55. Target collects the following information from consumers who use their credit and/or debit cards to make purchases at Target's stores:

> What Personal Information is Collected?
>
> Types of personal information we collect include:
>
> Your name
> Your mailing address
> Your e-mail address
> Your phone (or mobile) number
> Your drivers' license number
> Your credit/debit card number
> Your purchase/return/exchange information
> Your registry event information
> Your date of birth or age

Target, Privacy Policy, http://www.target.com/spot/privacy-policy (last visited Jan. 16, 2014).

56. Consumers' disclosure of PII is a condition of doing business with Target. Its Privacy Policy states: "If you choose not to provide personal information we may not be able to provide you with requested products, services or information." *Id.*

57. As described above, Target assures its consumers that it "maintain[s] administrative, technical and physical safeguards to protect [consumers'] personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information. *Id.*

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

58. As evidenced by the data breach described herein, Target failed to use industry standard methods to protect consumers' PII, both by failing to establish and maintain adequate safeguards, and by failing to timely notify Plaintiff and the Class of the data breach.

VI. CLASS ACTION ALLEGATIONS

59. Plaintiff brings this suit as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of herself and all others similarly situated, as members of a Class initially defined as follows:

> All customers in the United States of Target Corporation whose Personally Identifiable Information was compromised by Target's security breach(es) that occurred on or between November 27, 2013 and December 15, 2013, and any previous, subsequent or similar breaches.

60. Plaintiff also seeks to certify a Washington Subclass consisting of all members of the Class who are residents of Washington.

61. Numerosity. The Class is sufficiently numerous, as approximately 40 to 70 million (potentially up to 110 million) Target consumers have had their PII compromised. The Putative Class members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Putative Class members can be identified by records maintained by Defendant. Plaintiff alleges, upon information and belief, that Defendant has contacted and/or is in the process of contacting the approximately 40 to 70 million consumers whose PII was compromised as a result of the security breach.

62. Common Questions of Fact and Law. Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that predominate over any individual issues are:

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

(1) Whether Target failed to exercise reasonable care to protect Plaintiff's and the Class' PII;

(2) Whether Target timely, accurately, and adequately informed Plaintiff and the Class that their PII had been compromised;

(3) Whether Target's conduct with respect to the data breach was unfair and deceptive;

(4) Whether Target owed a legal duty to Plaintiff and the Class to protect their PII and whether Defendant breached this duty;

(5) Whether Target was negligent;

(6) Whether Target created a bargained-for promise to protect its consumers' PII that is supported by consideration;

(7) Whether Target retains consumers' data for a reasonable time;

(8) Whether Target breached this contractual obligation by failing to protect its consumers' PII;

(9) Whether Plaintiff and the Class are at an increased risk of identity theft as a result of Target's breaches and failure to protect Plaintiff's and the Class' PII; and

(10) Whether Plaintiff and members of the Class are entitled to the relief sought, including injunctive relief.

63. Typicality. Plaintiff's claims are typical of the claims of members of the Class because Plaintiff and the Class sustained damages arising out of Defendant's wrongful conduct as detailed herein. Specifically, Plaintiff's and the Class' claims arise from Target's failure to install and maintain reasonable security measures to protect Plaintiff's and the Class's PII, and to timely notify them when the security breach occurred.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

64. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class and has retained counsel competent and experienced in class action lawsuits. Plaintiff has no interests antagonistic to or in conflict with those of the Class and therefore is an adequate representative for Class.

65. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because the joinder of all members of the putative Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims asserted herein. There will be no difficulty in the management of this action as a class action.

VII. CAUSES OF ACTION

COUNT I: Negligence

66. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

67. Defendant had a duty to exercise reasonable care to protect and secure Plaintiff's and the Class' PII within its possession or control.

68. Defendant knew or should have known of industry standards and "best practices" of the industry when it came to protecting the private information of its consumers.

69. Defendant failed to take reasonable precautions to safeguard consumer PII, given the breaches involving other retailers, as noted above.

70. Through its acts and omissions described herein, Defendant unlawfully breached its duty to use reasonable care to protect and secure Plaintiff's and the Class' PII within its possession or control. More specifically, Defendant failed to maintain a number of reasonable security procedures and practices designed to protect the PII of Plaintiff and the Class, including,

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

but not limited to, establishing and maintaining industry-standard systems to safeguard its consumers' PII.

71. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and the Class have been harmed by the release of their PII, causing them to expend personal income on credit monitoring services and putting them at an increased risk of identity theft. Plaintiff and the Class have spent time and money to protect themselves as a result of Defendant's conduct, and will continue to be required to spend time and money protecting themselves, their credit, and their reputations.

COUNT II: Breach of Implied Contract

72. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

73. Defendant came into possession of Plaintiff's and the Class' PII for the purpose of selling merchandise to Plaintiff and the Class, and impliedly contracted with Plaintiff and the Class to protect such information. The contractual agreement specified that PII was a necessary to make purchases with credit and/or debit cards.

74. The terms of the contract, memorialized in Target's Privacy Policy, state that Target "use[s] industry standard methods to protect [consumers' PII]. Target, Privacy Policy, http://www.target.com/spot/privacy-policy (last visited Jan. 16, 2014).

75. Upon information and belief, Target failed to provide the level of security it promised to provide to its consumers to protect their PII.

76. Because Defendant failed to safeguard and protect Plaintiff's and the Class' PII according to industry standard methods, Defendant breached its contracts with Plaintiff and the Class.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

77. The duties breached by Target arise solely out of the terms of the implied contracts alleged *supra*.

78. Plaintiff and the Class suffered and will continue to suffer actual damages, including, but not limited to, the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

COUNT III: Breach of RCW 19.255.010
(Failure to Timely Disclose Breach of Security)

79. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

80. Defendant was aware of the security breach in which Plaintiff's and Class' PII was acquired by unauthorized persons as early as November 27, 2013 continuing through December 15, 2013.

81. Defendant has *never* notified Plaintiff of the security breach; however, Plaintiff was notified by the bank associated with her debit card. Moreover, upon information and belief, some members of the Class were notified as early as December 19, 2013, and others were notified as recently as January 16, 2014. Upon information and belief, Defendant has not yet notified all members of the Class of the security breach. Instead, Defendant is notifying members of the Class of the security breach on a rolling basis. As a result, not all members of Class have been notified.

82. Defendant was not prohibited from notifying Plaintiff and the Class of the security breach by any law enforcement agency.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

83. Defendant's failure to notify Plaintiff and the Class of the security breach without unreasonable delay in accordance with RCW 19.255.010 has and will delay Plaintiff and the Class from timely protecting and monitoring their PII from theft and unauthorized use.

84. As a result of Defendant's failure to notify Plaintiff and the Class according to Washington law, Plaintiff and the Class suffered and will continue to suffer actual damages, including, but not limited to, the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

COUNT IV: Violation Of The Washington Consumer Protection Act ("CPA") (RCW §§ 19.86 *et seq.*)

85. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

86. This claim arises under the Washington Consumer Protection Act, RCW §§19.86, *et seq.* ("CPA")

87. At all relevant times, Target engaged in "trade" and/or "commerce" within the meaning of RCW § 19.86.010.

88. The CPA broadly prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. RCW § 19.86.0120.

89. Target made uniform representations that it had taken adequate precautions to safeguard the PII of Plaintiff and the Class, even though it had not, and that it would continue to safeguard the PII, and, as set forth above, failed to timely disclose the security breach that compromised the PII, that, as set forth above, was unfair or deceptive, has and continues to have

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

the capacity to deceive the public, caused injury to Plaintiff and the Class, and was done in violation of the CPA.

90. In its communications and disclosures to Plaintiff and the Class, Target intentionally concealed and/or failed to disclose the security breach that occurred on or between November 27, 2013 and December 15, 2013 that compromised the PII of Plaintiff and the Class. This omission was unfair or deceptive, had and continues to have the capacity to deceive the public, caused injury to Plaintiff and the Class, and was done in violation of the CPA.

91. As set forth above, Target had unilateral knowledge that the security breach had occurred and that its consumers' PII was compromised, facts not known to Plaintiff or the Class. Target's exclusive knowledge of these material facts gave rise to a duty to disclose such facts, which it failed to perform.

92. The representations made by Target and the facts concealed and/or not disclosed by Target to Plaintiff and the Class are material facts that were likely to deceive reasonable consumers, and that a reasonable consumer would have relied on in safeguarding their PII.

93. The representations made by Target and the facts concealed and/or not disclosed by Target detrimentally affect the public interest. There is an inherent public interest in the truthful communication concerning consumers' PII. Target's inadequate safeguards of consumer PII and its delay and/or failure to timely notify consumers of the security breach compromised Plaintiff and the Class' PII, thereby negatively impacting the public interest.

94. Plaintiff and the Class justifiably acted or relied to their detriment on Target's affirmative representations and the concealed and/or non-disclosed facts as evidenced by their patronage of Target and failure to monitor their PII until notified by Target and/or, in some instances, as described with Plaintiff above, they were notified by their financial institution.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

95. Had Target taken reasonably adequate safeguards to protect its consumers PII and disclosed all material information regarding the security breach to Plaintiff and the Class, Plaintiff's and the Class' PII would not have been compromised and/or Plaintiff and the Class would have more timely monitored their PII following the security breach.

96. Target knew, or was reckless in not knowing, that the safeguards protecting their consumers' PII were insufficient and that its failure to timely notify its consumers about the security breach statements would cause harm to Plaintiff and the Class.

97. By the conduct described herein, Target engaged in unfair methods of competition and/or unfair or deceptive acts or practices in the conduct of business, trade or commerce.

98. As a direct and proximate result of Target's violations of the foregoing law, Plaintiff and the Class have been injured.

99. Plaintiff and the Class have been damaged and are entitled to all of the damages, remedies, fees, and costs available under the CPA.

100. Plaintiff and the Class will provide or already has provided any required notice to appropriate entities regarding Defendants' unfair and deceptive trade practices.

PRAYER FOR RELIEF

A. For an order certifying the Class herein under Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3) and appointing Plaintiff and Plaintiff's counsel of record to represent said Class;

B. Finding that Target breached its duty to safeguard and protect Plaintiff's and the Class' PII that was compromised in the security breach that occurred on or between November 27, 2013 and December 15, 2013;

C. Finding that Target breached its contracts with its consumers to protect their PII;

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

D. Awarding injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the Class for at least five years; (ii) the provision of bank monitoring and/or bank monitoring services for the Class for at least five years; (iii) the provision of identity theft insurance for the Class for at least five years; (iv) the provision of credit restoration services for the Class for at least five years; (v) awarding Plaintiff and the Class the reasonable costs and expenses of suit, including attorneys' fees, filing fees, and insurance for the Class; and (vi) requiring that Target receive periodic compliance audits by a third party regarding the security of its computer systems, specifically including laptops, used for processing and storing customer data, to ensure its compliance with federal and industry rules, regulations, and practices;

E. Awarding the damages requested herein to Plaintiff and the Class;

F. Awarding all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

G. Awarding pre-judgment and post-judgment interest as prescribed by law; and

H. Granting additional legal or equitable relief as this Court may find just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

DATED this 16th day of January, 2014.

KELLER ROHRBACK L.L.P.

By */s/ Lynn Lincoln Sarko*
Lynn Lincoln Sarko, WSBA # 16569
/s/ Gretchen Freeman Cappio
Gretchen Freeman Cappio, WSBA # 29576
/s/ Cari Campen Laufenberg
Cari Campen Laufenberg, WSBA # 34354
/s/ Karin B. Swope
Karin B. Swope, WSBA # 24015

KELLER ROHRBACK L.L.P.
1201 Third Ave., Suite 3200
Seattle, WA 98101
Tel: (206) 623-1900
Fax: (206) 623-3384
Email: lsarko@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com
kswope@kellerrohrback.com

Attorneys for Plaintiff

LAW OFFICES OF
KELLER ROHRBACK L.L.P.
1201 THIRD AVENUE, SUITE 3200
SEATTLE, WASHINGTON 98101-3052
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384